

## Table of Contents

<b>ELECTRONIC MAIL USE POLICY</b> .....	1
Introduction.....	1
General.....	1
Password Access Control.....	1
Message Storage and Deletion.....	1
Policy Violations.....	1
Policy Changes.....	2
Prohibited Usage and Prohibited Content List.....	2
<b>INTERNET USE POLICY</b> .....	3
Introduction.....	3
Internet Access.....	3
Acceptable/Unacceptable Uses.....	3
Data and Software Transmission.....	4
Policy Violations.....	4
Policy Changes.....	4
<b>ELECTRONIC CASE MANAGEMENT SYSTEM USE POLICY</b> .....	5
Access.....	5
Policy Violations.....	5
Policy Changes.....	5
<b>COMPUTER EQUIPMENT POLICY</b> .....	6
Policy Violations.....	6
Policy Changes.....	6
<b>APPENDIX A</b> .....	7

# **ELECTRONIC MAIL USE POLICY**

---

## **Introduction**

This document sets forth the Eastern Workforce Investment Board, Inc. (the "EWIB") policy regarding access to, monitoring, disclosure and proper use of EWIB internal and external electronic mail systems or other systems supported by EWIB ("Mail" or "Mail Systems"), messages and attachments sent or received by employees, contractors and consultants (collectively "Users"). It also includes the EWIB rules on the retention and destruction of electronic mail messages ("Messages") and attachments.

## **General**

- A. Use of the Mail Systems is not private. The EWIB may access, monitor, read, disclose and delete Messages at any time and for any reason without advance notice. This includes the creation, sending, receiving and storage of Messages to or from any internal or external source. The use of passwords or personal/custom named e-mail folders does not make such Messages private.
- B. The Mail Systems are necessary for EWIB business purposes. All Messages must be consistent with the Prohibited Usage and Prohibited Content List (see below), and all EWIB policies and procedures regarding ethical conduct, safety, compliance with applicable laws, and proper business practices.
- C. This Policy supersedes all other EWIB policies regarding access to and monitoring, disclosure and proper use of Mail Systems and Messages. This Policy is not meant to be exhaustive. Additional rules, procedures and guidelines regarding the use of Mail Systems and the treatment of Messages may be set forth in other EWIB policies and documents. However, in the event of an inconsistency, this Policy shall govern to the extent the issue falls within the scope of this policy.

## **Password Access Control**

- A. Each User is responsible for changing his or her password to help prevent unauthorized use of his/her user id. There are no password composition rules, however; use of complexity with passwords may help to eliminate misuse.
- B. Authorized EWIB Staff may change, bypass or disable a User's password or other security mechanisms at any time without permission of or advance notice to the User.

## **Message Storage Retention and Deletion**

Users should periodically remove unwanted Messages from their In-box, Sent Items and Deleted Items to maintain adequate levels of storage space unless expressly instructed by the EWIB Staff. Users are required to save Messages that are governed by the Oklahoma Open Records Act, State or Federal Regulations, or if subject to subpoena.

## **Policy Violations**

Employee Users who knowingly and willingly violate this Policy are subject to immediate discipline up to and including termination. Non-employee Users (e.g., contractors and consultants) are subject to immediate revocation of Mail System access and use privileges without notice. In addition to revocation, in the event a non-employee User violates this Policy, the EWIB may also exercise its rights under any applicable contract between the EWIB and the non-employee User or non-employee User's employer and any other rights the EWIB has under applicable law.

## **Policy Changes**

The EWIB reserves the right to change this Policy at any time without prior notice.

## **Prohibited Usage and Prohibited Content List**

The following list contains prohibited use of the EWIB's Mail Systems or other systems supported by EWIB and are considered a part of the EWIB E-mail Policy. If your desired use is not on the list, this does not mean it is permitted. All uses must be consistent with proper business practices and EWIB policies and procedures regarding ethical conduct, safety and compliance with applicable law. Users of EWIB Mail Systems or other systems supported by EWIB are strictly prohibited from:

- A. Intercepting, accessing, reading, or capturing by electronic means (commonly called "snooping") another User's Messages without prior permission (subject to the exceptions indicated elsewhere in this Policy or other EWIB policies or procedures);
- B. Using EWIB Mail Systems or other systems supported by EWIB to disseminate rumors, or false or misleading information;
- C. Falsely identifying themselves in Messages;
- D. Using profane, abusive, scandalous or threatening language or other inappropriate text in Messages;
- E. Creating, sending, forwarding or storing any content (including without limitation text, images, video, audio, and links thereto) that might violate the EWIB Sexual Harassment Policy or that might unreasonably interfere with an employees work performance;
- F. Reading incorrectly addressed Messages, except to the extent necessary to discover that a Message is incorrectly addressed (incorrectly addressed Messages can be forwarded to the intended recipient or to the EWIB Director);
- G. Using EWIB Mail Systems or other systems supported by EWIB to send e-mail to, or receive e-mail from a site to which access or use of the site, or the intended activity for which the e-mail is sent or received is (i) is restricted by the site owner, unless otherwise directed by authorized EWIB management or (ii) is prohibited by law or regulation;
- H. Bypassing the security mechanisms of EWIB Mail Systems;
- I. Deleting Messages or other EWIB records by electronic means in violation of the Oklahoma Open Records Act, State and Federal Regulations, or other EWIB policies or mandates issued by authorized EWIB management.

# **INTERNET USE POLICY**

---

## **Introduction**

The Internet is a worldwide conglomerate of private and public networks. Eastern Workforce Investment Board can significantly benefit from using the Internet through accessing and sharing business-related information. However, with this benefit come risks, including security, inconsistent performance, difficulty in locating information and misuse of employee time. To mitigate these risks, the Eastern Workforce Investment Board's Internet Use Policy formally documents the rules for Internet access and use.

## **Internet Access**

Internet access must only be provided to employees, consultants or contractors with a business need. Each user must understand the risks of Internet use and adhere to the information security policies outlined below. Each user must also adhere to all Eastern Workforce Investment Board's Operating Policies, State or Federal Regulations, and the Eastern Workforce Investment Board Code of Conduct.

Authorized EWIB Staff must approve each user access request. The authorized EWIB staff must understand the purpose of the request, exercise appropriate judgment regarding the risks associated with Internet access, and approve access only for those employees, consultants or contractors who have a legitimate business need. In addition, the authorized EWIB staff should perform periodic validation of user access.

The inherent insecurity of the Internet requires implementation of firewalls to protect computers and internal networks from unauthorized access. The EWIB or other systems supported by EWIB connection to the Internet is secured through a service provider's firewall and is the only acceptable method of connection. All other direct connections must be disabled.

The Internet connection must not be used to access other computers without the permission of the owner (i.e., explicit permission or implied by customary guest or anonymous access used throughout the Internet community). EWIB users of the Internet are expected to be responsible in their use of the network and avoid actions that cause interference or disruption to the network or to the work of others on the network.

## **Acceptable/Unacceptable Uses**

Users of the Internet may be subject to monitoring in several respects including unauthorized access attempts and improper content. Users should understand and recognize that the content of Internet messages and other transmissions are not private. EWIB authorized staff may monitor and read any and all such transmissions.

Examples of Acceptable uses of the Internet may include\*:

- Transmission of business-related electronic mail
- Retrieval of documents and program corrections from vendors or other service providers
- Retrieval of stock market, economic, or other industry-related information
- Retrieval of business-related research and education.

Examples of Unacceptable uses of the Internet may include\*:

- Transmission of information in violation of any state, federal or international laws or regulations.
- Usage of prohibited sites which may include but are not limited to, sites whose purpose is to convey information about Any one of the following:
  - Gambling, Hate, Sale and/or Manufacturing of Illegal Drugs, Pornography, Obscenity, or Terrorism.

\*Eastern Workforce Investment Board reserves the right to amend this section of the policy and identify additional acceptable or unacceptable uses.

### **Data and Software Transmission**

Copyrighted and licensed software must not be duplicated unless duplication is expressly allowed in writing within the software. Freeware or shareware originating from the Internet **MUST NOT** be used within EWIB networks or other systems supported by EWIB unless approved in advance by Management. Users should be aware that information on the Internet may be fabricated, misleading or stolen. Free programs may contain viruses or trojan horses, designed to destroy or acquire information.

Software retrieved from the Internet should not be allowed to operate on any EWIB internal network or other systems supported by EWIB until it has been thoroughly tested and checked for potentially damaging code through a standard virus scanning process on the receiving stand-alone system.

### **Policy Violations**

EWIB employees who knowingly and willingly violate the EWIB Internet Use Policy may be subject to disciplinary action up to and including termination. In the case of non-employee users, violation may lead to removal of access to EWIB systems, EWIB Internet connections or other systems supported by EWIB. In addition to revocation, the EWIB may also exercise its rights under any applicable contract between the EWIB and the non-employee User or non-employee User's employer and any other rights the EWIB has under applicable law. Furthermore, in the event of an illegal activity, the user will also be reported to the appropriate law enforcement authority.

### **Policy Changes**

The EWIB reserves the right to change this Policy at any time without prior notice.

## **ELECTRONIC CASE MANAGEMENT SYSTEM USE POLICY**

---

Users of the Electronic Case Management System must abide by the following:

- Users may only use the Electronic Case Management System for the specific functions for which have been authorized and for official agency business. These resources are not to be used for personal use or personal gain.
- Information concerning customers, employers, and employees in the custody of the Electronic Case Management System is confidential and may not be accessed, viewed, copied, printed, distributed, disclosed or otherwise manipulated unless it is needed to perform official duties. Information should not be re-disclosed to anyone outside of the agency except to the individual who is the subject of the information.
- Passwords are confidential and may not be written down and are to be used only by the User. Computers left unattended must have screens clear of any confidential information. Failure to do so exposes the information to unauthorized users, and the User may be held responsible for their actions.
- Records in the custody of the Electronic Case Management System must not be deleted by electronic or other means in violation of the Oklahoma Open Records Act, State and Federal Regulations, or other EWIB policies or mandates issued by EWIB.

### **Access**

The Oklahoma Employment Security Commission will approve each user's access request to the Electronic Case Management System based upon recommendation from the EWIB staff. Authorized EWIB Staff must set security access levels for each user. The authorized EWIB staff must understand the purpose of the request, exercise appropriate judgment regarding the risks associated with Internet access, and approve access only for those employees, consultants or contractors who have a legitimate business need. In addition, the authorized EWIB staff should perform periodic validation of user access.

### **Policy Violations**

EWIB employees who knowingly and willingly violate this policy may be subject to disciplinary action up to and including termination. In the case of non-employee users, violation may lead to removal of access to the Electronic Case Management System. In addition to revocation, the EWIB may also exercise its rights under any applicable contract between the EWIB and the non-employee User or non-employee User's employer and any other rights the EWIB has under applicable law. Furthermore, in the event of an illegal activity, the user will also be reported to the appropriate law enforcement authority.

### **Policy Changes**

The EWIB reserves the right to change this Policy at any time without prior notice.

## **COMPUTER EQUIPMENT POLICY**

---

To ensure optimum computer performance, regularly scheduled maintenance must be performed on all EWIB owned computers. See Appendix A. In the event that maintenance does not correct the problem, EWIB staff will diagnose and attempt to repair the equipment. The non-employee User or the non-employee Users' employer should not attempt to repair EWIB owned equipment unless directed to do so by authorized EWIB staff.

An anti-virus program will be provided for each EWIB owned computer. This program should not be disabled except for software installation. The latest virus definitions must be obtained for the anti-virus program when they are available.

EWIB owned equipment must not be removed from its premises or within the premises without the authorization of the EWIB Executive Director. Inventory control tags must not be removed from any EWIB owned equipment except in the case of salvage.

### **Policy Violation**

EWIB employees who knowingly and willingly violate this policy may be subject to disciplinary action up to and including termination. Damage resulting from abuse, misuse, or neglect to EWIB owned equipment may lead to removal of the Users access to such equipment. In addition to revocation, in the case of non-employee users, the EWIB may also exercise its rights under any applicable contract between the EWIB and the non-employee User or the non-employee User's employer and any other rights the EWIB has under applicable law. Furthermore, in the event of an illegal activity, the user will also be reported to the appropriate law enforcement authority.

### **Policy Changes**

The EWIB reserves the right to change this Policy at any time without prior notice.

### Computer Maintenance Options

#### Disk Cleanup

Disk Cleanup helps free up space on your hard drive. Disk Cleanup searches your drive, and then shows you temporary files, Internet cache files, and unnecessary program files that you can safely delete. You can direct Disk Cleanup to delete some or all of those files.

Open Disk Cleanup.

- To open Disk Cleanup, click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Disk Cleanup**.

#### Detecting and repairing disk errors

You can use the Error-checking tool to check for file system errors and bad sectors on your hard disk.

1. Open My Computer, and then select the local disk you want to check.
  2. On the **File** menu, click **Properties**.
  3. On the **Tools** tab, under **Error-checking**, click **Check Now**.
  4. Under **Check disk options**, select the **Scan for and attempt recovery of bad sectors** check box.
- To open My Computer, click **Start**, and then click **My Computer**.
  - All files must be closed for this process to run. If the volume is currently in use, a message box will appear prompting you to indicate whether or not you want to reschedule the disk checking for the next time you restart your system. Then, the next time you restart your system, disk checking will run. Your volume will not be available to perform other tasks while this process is running.
  - If your volume is formatted as NTFS, Windows automatically logs all file transactions, replaces bad clusters, and stores copies of key information for all files on the NTFS volume

#### Disk Defragmenter

You might need to be logged on as an administrator or a member of the Administrators group in order to perform some tasks.

Disk Defragmenter consolidates fragmented files and folders on your computer's hard disk, so that each occupies a single, contiguous space on the volume. As a result, your system can gain access to your files and folders and save new ones more efficiently. By consolidating your files and folders, Disk Defragmenter also consolidates the volume's free space, making it less likely that new files will be fragmented.

Open Disk Defragmenter.

- To open Disk Defragmenter, click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Disk Defragmenter**.
- For information about using Disk Defragmenter, on the **Action** menu in Disk Defragmenter, click **Help**.

## **Backup**

The Backup utility helps you create a copy of the information on your hard disk. In the event that the original data on your hard disk is accidentally erased or overwritten, or becomes inaccessible because of a hard disk malfunction, you can use the copy to restore your lost or damaged data.

Open Backup.

- To start Backup, click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
- The Removable Storage service must be started for Backup to work properly. You can also use the Automated System Recovery Wizard in the Backup utility to help you repair your system.

## **Viruses and Trojan horses**

In today's computing world, you must prevent intentional intrusions into your computer and network that take the form of viruses and Trojan horses. EWIB will provide virus-detection software for all EWIB owned computers. Please inform the EWIB staff before your virus subscription expires. Follow these tips to help prevent virus outbreaks and Trojan horse attacks.

- Educate yourself about viruses and how they are commonly spread. You can unwittingly bring viruses into the network by loading a program from a source such as the Internet, online bulletin board, or e-mail attachments.
- Learn the common signs of viruses: unusual messages that appear on your screen, decreased system performance, missing data, and inability to access your hard drive. If you notice any of these problems on your computer, run your virus-detection software immediately to minimize the chances of losing data.
- Programs on floppy disks may also contain viruses. Scan all floppy disks before copying or opening files from them, or starting your computer from them.
- Be sure to obtain the latest virus definitions for your program when they are available, because new viruses are created every day.

The following is a well-known on-line tool that can help you detect and remove viruses from your computer: <http://www.antivirus.com>

## **Windows Update**

You might need to be logged on as an administrator or a member of the Administrators group in order to perform some tasks.

Windows Update is the online extension of Windows that helps you keep your computer up to date. Microsoft offers important updates, which include security and other critical updates, to help protect your computer against new viruses and other security threats that can spread over the Internet or a network. Other updates contain enhancements such as upgrades and tools that can help your computer run more smoothly. Windows Update scans your computer and

provides you with a tailored selection of updates that apply only to the software and hardware on your computer.

To find available updates

1. Open Windows Update.
  2. On the Windows Update home page, click **Scan for Available Updates**.
- To open Windows Update, click **Start**, click **All Programs**, and then click **Windows Update**.
  - The first time you go to the Windows Update Web site, click **Yes** when prompted to install any required software or controls.
  - To use Windows Update, you need to establish a connection to the Internet.

### Scheduled Tasks

1. Open Scheduled Tasks.
  2. Double-click **Add Scheduled Task**.
  3. Follow the instructions in the Scheduled Task Wizard.
- To open Scheduled Tasks, click **Start**, click **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Scheduled Tasks**.
  - If you want to configure advanced settings for the task, select the **Open advanced properties for this task when I click Finish** check box on the final page of the wizard.
  - Confirm that the system date and time on your computer are accurate, because Scheduled Tasks relies on this information to run scheduled tasks. To verify or change this information, double-click the time indicator on the taskbar.
  - If you leave the password blank and you want the task to run when you are logged on, open the task. On the **Task** tab, select the **Run only if logged on** check box. The task will run at its scheduled time when the user who created the task is logged on to the computer.

### SPYWARE

Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent. You might have spyware or other unwanted software on your computer if:

- You see pop-up advertisements even when you're not on the Web.
- The page your Web browser first opens to (your home page) or your browser search settings have changed without your knowledge.
- You notice a new toolbar in your browser that you didn't want, and find it difficult to get rid of.
- Your computer takes longer than usual to complete certain tasks.
- You experience a sudden rise in computer crashes.

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. These programs have the ability to change your Web browser's home page or search page, or add additional components to your browser you don't need or want. These programs also make it very difficult for you to change your settings back to the way you originally had them. These types of unwanted programs are also often called spyware.

### **Spyware Removal**

1. Download one of the free removal tools listed below and install it.
2. Run the tool to scan your computer for spyware and other unwanted software.
3. Review the files discovered by the tool for spyware and other unwanted software.
4. Select suspicious files for removal by following the tool's instructions.

The following are a few well-known tools that can help you detect and remove unwanted software from your computer

Lavasoft Ad Aware: <http://www.lavasoft.de/ms/index.htm>

Spybot Search & Destroy (S&D): <http://www.safer-networking.org/microsoft.en.html>

Other tools are available at: [http://www.download.com/Spyware-Center/2001-2023\\_4-0.html?tag=dir](http://www.download.com/Spyware-Center/2001-2023_4-0.html?tag=dir)